
The following is a complete listing of the pending claims:

1. (Original) A device for controlling access to a resource, access being provided through a host device having a USB bus, the device comprising:
 - (a) an input for receiving a request to access the resource;
 - (b) a flash memory device for storing at least one permission for determining access to the resource;
 - (c) a flash memory controller for controlling said flash memory device;
 - (d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided; and
 - (e) a USB interface controller for communicating with the USB bus of the host device and, if permitted, for transmitting data from said processor.
2. (Original) The device of claim 1, wherein the device is implemented as a programmable ASIC.
3. (Original) The device of claim 1, wherein access is determined according to a biological parameter of a user, the device further comprising a biometric detection device for detecting said biological parameter of the user and for determining whether the user has said at least one permission to access the stored data, said biometric detection device being connected to said processor.

4. (Original) The device of claim 3, wherein said biometric detection device further comprises:

- (i) a sample collector for collecting said biological parameter of the user; and
- (ii) a software module for analyzing said biological parameter to determine whether the user has said at least one permission to access the resource.

5. (Original) The device of claim 4, wherein said biometric detection device further comprises:

- (iii) a memory device for storing said software module and at least one previously collected biological parameter of the user; and
- (iv) a data processor for operating said software module.

6. (Original) The device of claim 5, wherein said biological parameter of the user is a fingerprint of the user.

7. (Original) The device of claim 1, further comprising:

- (f) a RAM component for storing data for performing said at least one instruction of said data processor.

8. (Original) The device of claim 1, further comprising:

- (f) a cryptographic chip for encrypting and decrypting data.

9. (Original) The device of claim 8, wherein said cryptographic chip performs an authentication process.

10. (Original) The device of claim 8, wherein said cryptographic chip emulates a smart card.

11. (Original) The device of claim 10, wherein said cryptographic chip stores encrypted smart card data.

12. (Original) The device of claim 8, wherein said cryptographic chip performs encryption immediately upon receiving a command from said data processor.

13. (Original) The device of claim 12, wherein said cryptographic chip creates a cryptographic signature with a hash immediately upon receiving a command from said data processor.

14. (Original) The device of claim 8, wherein said cryptographic chip further comprises a cryptographic chip memory for storing at least one cryptographic key and at least one cryptographic instruction for encrypting and decrypting data, such that said cryptographic chip forms a removable encryption engine.

15. (Original) The device of claim 14, wherein said encrypted data is stored on said cryptographic chip memory.

16. (Original) The device of claim 15, wherein said cryptographic chip memory is a separate flash memory device from said flash memory device.

17. (Original) The device of claim 15, wherein said cryptographic chip memory is said flash memory device.

18. (Withdrawn) A system for controlling access to a network resource, the system comprising:

- (a) an active data device for controlling access to the network resource, said active data device featuring a USB (universal serial bus) interface controller;
- (b) a host computational device for communicating with said active data device to provide access to the network resource, said host computational device featuring a USB bus for communicating with said USB interface controller for data exchange with said active data device; and
- (c) a network for connecting said host computational device to the network resource.

19. (Withdrawn) The system of claim 18, wherein said active data device further comprises firmware for storing a plurality of instructions and a data processor for performing said plurality of instructions, such that said active data device determines said access according to said instructions of said firmware.

20. (Withdrawn) The system of claim 18, wherein said active data device is implemented as a programmable ASIC.

21. (Withdrawn) The system of claim 18, wherein said active data device further comprises:

- (i) a non-volatile memory for storing at least one instruction for determining access to the network resource; and
- (ii) a processor for executing said at least one instruction to determine if access is to be provided to the network resource.

22. (Withdrawn) The system of claim 21, wherein said non-volatile memory is a flash memory device, such that said active data device further comprises a flash controller for being controlled by said processor.

23. (Withdrawn) The system of claim 18, wherein access is determined according to a biological parameter of a user and said active data device further comprises a biometric detection device for detecting said biological parameter of the user and for determining whether said user has permission to access the network resource.

24. (Withdrawn) The system of claim 23, wherein said biometric detection device further comprises:

- (i) a sample collector for collecting said biological parameter of the user; and

-
- (ii) a software module for analyzing said biological parameter to determine whether said user has said permission.

25. (Withdrawn) The system of claim 24, wherein said biometric detection device further comprises:

- (iii) a memory device for storing said software module and at least one previously collected biological parameter of the user; and
- (iv) a data processor for operating said software module.

26. (Withdrawn) The system of claim 25, wherein said biological parameter of the user is a fingerprint of the user.

27. (Withdrawn) The system of claim 18, further comprising:

- (d) a cryptographic chip on said active device for encrypting and decrypting data, such that access to said host computational device is determined according to an authentication procedure performed with said cryptographic chip.

28. (Withdrawn) A method for controlling access to a resource, access being provided through a host device having a USB bus, the method comprising the steps of:

- (a) providing an active data device for determining access to the resource, said active data device featuring an USB interface controller;
- (b) receiving a request to access the resource by said active data device;

-
- (c) comparing said request to at least one permission for determining access to the resource by said active data device;
 - (d) if said at least one permission includes a type of access requested in said request, sending said request from said active data device to the USB bus of the host device through said USB interface controller;
 - (e) providing access to the resource through the host device; and
 - (f) alternatively, if said at least one permission does not include said type of access requested in said request, rejecting said request by said active data device.

29. (Withdrawn) The method of claim 28, wherein access is determined for a user and wherein step (b) further comprises the steps of:

- (i) collecting a biological parameter of said user; and
- (ii) analyzing said biological parameter to determine an identity of said user, such that said at least one permission is determined according to said identity.

30. (Withdrawn) A device for controlling access to a resource, access being provided through a host device having a radio transceiver, the device comprising:

- (a) an input for receiving a request to access the resource;
- (b) a flash memory device for storing at least one permission for determining access to the resource;
- (c) a flash memory controller for controlling said flash memory device;

-
- (d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, access to the resource is provided, and alternatively if said at least one permission does not include a type of access requested in said request, access to the resource is not provided;
 - (e) a device radio transceiver for communicating with the radio transceiver of the host device and, if permitted, for transmitting data from said processor; and
 - (f) a radio transceiver interface controller for controlling said device radio transceiver.

31. (Withdrawn) The device of claim 30, wherein said radio transceiver is implemented according to Bluetooth technology.

32. (Withdrawn) A system for controlling access to a network resource, the system comprising:

- (a) an active data device for controlling access to the network resource, said active data device featuring a device radio transceiver;
- (b) a host computational device for communicating with said active data device to provide access to the network resource, said host computational device featuring a radio transceiver for communicating with said device radio transceiver for data exchange with said active data device; and

-
- (c) a network for connecting said host computational device to the network resource.

33. (Withdrawn) The system of claim 32, wherein said radio transceiver is implemented according to Bluetooth technology.

34. (Withdrawn) A system for controlling access to stored data, the system comprising:

- (a) an electronic data storage device for storing the stored data; and
- (b) an access control device for controlling access to said electronic data storage device, such that the stored data is only accessed through said access control device, and such that said access control device determines access to the stored data according to at least one permission.

35. (Withdrawn) The system of claim 34, wherein said data storage device and said access control device are implemented as a plurality of separate components.

36. (Original) The system of claim 34, wherein said access control device further comprises:

- (i) an input for receiving a request to access the stored data;
- (ii) a non-volatile memory for storing at least one permission for determining access to the stored data;

-
- (iii) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and
 - (iv) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.

37. (Withdrawn) The system of claim 36, wherein said non-volatile memory is a flash memory device.

38. (Original) The system of claim 37, further comprising:
- (c) a CPU (central processing unit) for transmitting said request to said access control device and for receiving provided data; and
 - (d) a bus for connecting said CPU to said access control device, such that said electronic data storage device is not accessed through said CPU, but only through said access control device.

39. (Withdrawn) The system of claim 38, wherein said bus is a USB (universal serial bus).

40. (Withdrawn) The system of claim 39, wherein said at least one permission is for comparing said request to the stored data and for returning a positive

or negative comparison, such that if said request is identical to the stored data, said comparison is positive, and alternatively such that if said request is not identical to the stored data, said comparison is negative, and such that the stored data is not read.

41. (Withdrawn) The system of claim 34, further comprising:
 - (c) an MP3 player for playing MP3 file data; and
 - (d) an MP3 interface for said access control device, said MP3 interface enabling said access control device to communicate with said MP3 player to determine access to said MP3 file data.
42. (Original) A device for controlling access to data stored in an electronic data storage device, the device comprising:
 - (a) an input for receiving a request to access the stored data;
 - (b) a non-volatile memory for storing at least one permission for determining access to the stored data;
 - (c) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and
 - (d) a processor for executing said at least one instruction and for comparing said request to said at least one permission, such that if said at least one permission includes a type of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.

43. (Withdrawn) A method for controlling access to data stored in an electronic data storage device, the method comprising the steps of:

- (a) providing an access control device for determining access to the electronic data storage device;
- (b) receiving a request to access the stored data by said access control device;
- (c) comparing said request to at least one permission for determining access to the stored data by said access control device;
- (d) if said at least one permission includes a type of access requested in said request, performing said request for accessing the stored data from the electronic data storage device by said access control device; and
- (e) alternatively, if said at least one permission does not include said type of access requested in said request, rejecting said request by said access control device.

44. (Withdrawn) The method of claim 43, wherein said type of access includes permission to read from the stored data, such that step (d) includes the step of reading from the stored data.

45. (Withdrawn) The method of claim 44, wherein said type of access includes permission to write to the stored data, such that step (d) includes the step of writing to the stored data.

46. (Withdrawn) The method of claim 43, wherein said type of access only includes comparing said request to the stored data and for returning a positive or

negative comparison, such that if said request is identical to the stored data, step (d) includes the step of returning a positive comparison, and alternatively such that if said request is not identical to the stored data, step (d) includes the step of returning a negative comparison, such that the stored data is not read.

47. (Withdrawn) The method of claim 43, wherein the stored data is a credit card number, and said credit card number features a plurality of types of data, each of said plurality of types of data being stored with a separately selected access permission.

48. (Withdrawn) The method of claim 43, wherein the stored data has a permission for a predetermined number of data read accesses, such that step (c) includes the steps of:

- (i) determining a number of performed data read accesses for the stored data; and
- (ii) if said number of performed data read accesses is less than said predetermined number of data read accesses, permitting the stored data to be read.

49. (Withdrawn) The method of claim 43, wherein access is determined for a user and wherein step (b) further comprises the steps of:

- (i) collecting a biological parameter of said user; and
- (ii) analyzing said biological parameter to determine an identity of said user, such that said at least one permission is determined according to said identity.

50. (Withdrawn) A device for controlling access to data stored in an electronic data storage device by a user, access being determined according to a biological parameter of the user, the device comprising:

- (a) a biometric detection device for detecting said biological parameter of the user and for determining whether the user has said at least one permission to access the stored data;
- (b) an input for receiving a request to access the stored data;
- (c) a non-volatile memory for storing at least one permission for determining access to the stored data;
- (d) at least one instruction for determining a permitted access according to the at least one permission, said at least one instruction being stored on said non-volatile memory; and
- (e) a processor for executing said at least one instruction and for comparing said request to said at least one permission, said processor being connected to said biometric detection device, such that if said at least one permission includes a type of access requested in said request, the stored data is provided, and alternatively if said at least one permission does not include a type of access requested in said request, the stored data is not provided.